

**Navy Playbook**  
for  
***Response to Release of Navy  
Personnel's Personally Identifiable  
Information (PII)***



## Preface

---

4 May 2015

In March 2015, the Islamic State of Iraq and the Levant (ISIL) and/or its supporters posted online the names and addresses of 100 Department of Defense personnel, of whom 41 were associated with the Department of Navy. The information gathered was easily obtainable from Internet searches and social media. We should expect that the posting of such publically available information will continue.

While we serve in the greatest Navy the world has ever known, risk is a part of our profession. We cannot eliminate risk, but we can take steps to mitigate it through training, education and awareness of our surroundings. This training must also be shared with our family members as well so that they can live smart, not scared.

This Playbook provides Navy leaders, Commanders and Commanding Officers with:

- Procedures for notification of individuals who have their personal information posted online
- Home and family security tips, and an Individual Security Vulnerability Assessment Checklist to help affected personnel determine if they have security vulnerabilities at home
- Links to NCIS resources to help Navy personnel manage Personal, Residence, Vehicle, Office, and Cybersecurity risks
- A link to online Antiterrorism/Force Protection Level 1 training that family members are able to take without a Common Access Card (CAC)
- A link to Department of Defense resources on managing Social Media
- Talking points for addressing this issue with various audiences (Sailors and Department of Navy civilians, families, the media, etc.)

This Playbook is intended for distribution to all echelon 2 commands, Flag Officers, Commanders and Commanding Officers to ensure that leaders understand our notification process and have the resources they need to educate their personnel on this matter.



S. H. SWIFT

Vice Admiral, U.S. Navy

Director, Navy Staff

**Title:** Response to Release of Navy Personnel's Personally Identifiable Information (PII)

**Audience for the Playbook:** Navy leaders, Commanders, Commanding Officers

### **Purpose**

---

To provide Navy leaders, Commanders and Commanding Officers with guidance on notification and support to assigned personnel and their families in the event that their PII has been publicly released by an international organization such as the Islamic State in Iraq and the Levant (ISIL), or their sympathizers.

Adversaries have leveraged our social media footprint to create fear and anxiety among our Sailors, civilian employees and their families. This playbook outlines the procedures to be implemented in response to any further release of PII.

All actions in support of our response should be:

- Coherent
  - Relatable to the threat
  - Scalable
- Consistent
  - Over time
- Congruent
  - Across services
- Concise
  - Repeatable at all ranks
  - Shared internally and externally

### **Core Message**

---

Commanders and Commanding Officers are responsible for contacting and providing follow-on support to Service members who have had their PII publicly released in an attempt to intimidate or otherwise threaten them and their families.

We should expect that the posting of publically available information of Navy personnel will continue. Department of Defense and Naval Criminal Investigative Service (NCIS) have not found evidence of operational planning or an imminent threat to individuals who have had their PII posted online, to date.

Navy is coordinating with NCIS to determine the full range of potential actions to be taken in the event that NCIS and/or other agencies have evidence that an individual whose personal

information has been posted is being targeted. We are also assessing the long term implications to our personnel of these lists residing on the internet for extended periods.

OPNAV N3/N5 is in close communication with NCIS and will provide updates to echelon 2 commands as additional information becomes available.

## Contents

---

<b>Notification Process</b>	<b>6</b>
<b>Initial Contact Script</b>	<b>7</b>
<b>Example Talking Points</b>	<b>9</b>
<b>Sample Questions and Answers</b>	<b>13</b>
<b>Follow-on Support</b>	<b>14</b>
<b>Home and Family Security Tips</b>	<b>15</b>
<b>Operations Security Guidance for Family Members</b>	<b>19</b>
<b>Individual Security Vulnerability Assessment Checklist</b>	<b>21</b>

## Notification Process

---

The NCIS Multiple Threat Alert Center (MTAC), or other law enforcement / Intelligence Community source, will provide initial notification to Navy via the CNO Navy Operations Center (NOC) in the event of a PII release affecting Navy personnel. This notification will be provided after MTAC has had an opportunity to assess the origin of the list and determine the necessary resources required to complete military affiliation checks for named individuals. At the time of initial NOC notification, MTAC will also provide an estimated time in which the list review will be completed and provided.

NCIS will confirm the identities of the DON personnel whose PII has been posted online and provide the NOC with the names and assigned commands of the affected active duty, reserve force and Department of Navy (DON) government civilian personnel. Retired personnel and DON contractors affected by the release will be notified directly by NCIS but will not receive a follow-on brief. The FBI will contact any other personnel who have separated from the Navy.

- NCIS will assess the credibility of the threat to the Service member or DON government civilian employee and will provide the assessment to the NOC.
- NCIS will directly notify a Service member or government civilian employee if they deem that there is a credible and imminent threat to the individual and/or their family, or if the individual's name is associated with an ongoing criminal investigation. NCIS will notify the NOC Watch Officer and advise them of any actions taken as soon as practicable thereafter.
- NCIS Field Offices will provide the MTAC with updates on the notification status of retired personnel and DON contractors.

The NOC will notify affected echelon 2 command Maritime Operations Centers or Command Duty Officers.

- Echelon 2 commands will direct subordinate commands to notify affected members. Affected personnel will be notified by either a telephone call or in person within 24-hours of NOC receipt of the NCIS-reviewed list.
- Commands will provide information as described in the Initial Contact Script section of the Handbook.
- Follow-on contact will be offered and scheduled if desired by the Service member, government civilian, or dependent. Follow-on contact should be conducted per the Follow-on Support section of this Playbook.
- Command representatives will report results of contact via their chain of command. Echelon 2 commands will provide the NOC with updates on the status of initial notifications at 0200 EST and 1400 EST daily until all notifications are completed.
- Any information regarding suspicious activity noted by the affected Sailor, DON government civilian employee or family members gleaned during the initial notification or follow-on briefing shall be immediately reported by the command to the supporting NCIS field office.
- The affected individual's command is responsible for contacting the NCIS Field Office for any additional support after the individual has been notified.

## Initial Contact Script

---

### Introduction

The Navy, working with Federal law enforcement agencies, closely monitors any threats to the safety and well-being of Department of Navy members and their families. In the recent past, terrorist organizations have released Personally Identifiable Information (PII) as a tactic to harass or intimidate Navy members while at the same time calling upon unknown sympathizers to undertake violent action.

### Assessment

We have just learned that your PII has been released online by a group claiming affiliation with a terrorist organization. The group may have acquired your information via publically available online news stories, websites, or social media accounts.

The following information about you was released:

- ☐ Name
- ☐ DoD Affiliation
- ☐ Social Security Number
- ☐ Date of Birth
- ☐ Phone Number
- ☐ Address
- ☐ Social media user I.D.
- ☐ Other \_\_\_\_\_

There is currently no information to suggest that there is any ongoing planning to specifically target you or your family. However, we cannot rule out the possibility that someone unknown to us might attempt to use this publicly available PII for illegal purposes. If law enforcement authorities become aware of any additional indication that you are in danger, we will notify you. In the meantime, because of the risk associated with the public exposure of your PII, we recommend you take the following actions:

### Recommendations

If you notice anything suspicious that makes you feel threatened, call 911 or your local emergency services immediately. Make a secondary notification to NCIS and your command.

If you notice anything suspicious that is not immediately threatening, notify NCIS and Command as soon as possible.

Examples of threatening or suspicious activity include:

- Suspicious vehicle or individual(s) around your neighborhood or residence.
- Threats (in person, telephonic or online.)

- You are approached or questioned by suspicious individual(s).
- Online or electronic solicitations from individuals seeking to acquire information about you or any online account you may have

Review all of your online and social media activity and ensure all of your account settings are set to private. Remove any information that publically identifies your military affiliation or personally identifiable information.

**Provide the service member with the following:**

- A copy of or link to the NCIS Threat Management Security Recommendations brochure and the Staying Safe PowerPoint Brief that addresses management of Personal, Residence, Vehicle, Office, Social media and Cybersecurity risks. These documents provide simple tips that Service members can use to enhance their security. They are located at the following address as the "Safety Recommendations Brochure" and "Stay Safe PowerPoint Brief":  
<http://www.ncis.navy.mil/CoreMissions/CI/Pages/default.aspx>
- The link to the Defense Media Activity Guide to Keeping Your Social Media Accounts Secure:  
[http://www.defense.gov/documents/WEB Guide to Keeping Your Social Media Accounts Secure 2015.pdf](http://www.defense.gov/documents/WEB%20Guide%20to%20Keeping%20Your%20Social%20Media%20Accounts%20Secure%202015.pdf)
- A copy of the link to Anti-Terrorism/Force Protection Level 1 training:  
<http://jko.jten.mil/courses/at1/launch.html>
- A copy of the following:
  - Home and Family Security Tips (page 15)
  - Operations Security Guidance for Family Members (page 19)
  - An Individual Security Vulnerability Assessment Checklist (page 21)

If notification is conducted by telephone, offer and schedule a face-to-face brief if desired.

**Reiterate to the Service member that they will be re-contacted if anything changes or new intelligence becomes available.**

**Provide the following contact information:**

Local Emergency Services: 911

Local Police Department:

Base Police:

Local NCIS Office:

Command Representative:

## Talking Points

---

### Internal Communication Efforts

U.S. Navy leaders are strongly encouraged to take time to discuss this issue (and social media safety) with their Sailors and civilian personnel. Placing this issue into its appropriate context will help ease anxiety and focus responsive effort on productive, appropriate and necessary measures.

### Office of the Secretary of Defense (OSD) Talking Points

#### Points for Use with the Public/Media

- ISIL represents a serious and complex threat, and continues to use social media in an effort to intimidate its enemies.
- This most recent attempt by ISIL to incite attacks against U.S. military personnel is an example of the threats faced by members of our military.
- (If True) The services are conducting appropriate individual notifications in accordance with their service-specific procedures.
- (If True) At this time, we are not aware of operationalized or imminent threats linked to these statements.
  - The safety and security of our service members and their families is one of DoD's primary concerns.
  - We are not going to discuss specific force protection measures.
- We continue to work closely with our partners in the law enforcement and intelligence communities to mitigate the threat posed by ISIL.
- We remain focused on Homegrown Violent Extremists (HVEs), particularly those who may sympathize with and act on ISIL's message.
- The majority of the information disclosed by ISIL in the past was taken from publically accessible websites and social media platforms.
- There are common sense steps individuals can take to limit their vulnerability online.
- We encourage everyone to consider the content they post online and on websites and social media platforms accessible to the public such as Facebook, Twitter, and LinkedIn.
- It is important that everyone verifies his/her privacy settings on their social media sites to protect personal information.

#### Military Family Emphasis Points

- The safety and security of our service members and their families is one of DoD's primary concerns.
- (If True) The services are conducting appropriate individual notifications in accordance with their service-specific procedures.
- In response to the March disclosure, to reduce the risk and vulnerability of potential targeting or terrorist attack, USNORTHCOM and USPACOM issued force protection advisories to provide security awareness information to Service members, their Families, DoD civilians, and contractor personnel

- Service members should consult their Component's published social media guidance to help improve online security practices.
- There are certain details of your personal lives that should never be made public as they could pose concern for you, your family, or the Department.
  - Avoid sharing information that may someone to predict or track where you or your family might be such as your home addresses, phone numbers, times and locations of events you plan to attend, where your children go to school, etc.

#### Congressional Emphasis Points

- We remain committed to ISIL's degradation and eventual defeat while ensuring the safety of our Service members and their Families. The security of our people is one of DoD's highest concerns.
- We remain focused on the danger posed by HVEs who are sympathetic to ISIL messaging and who may be incited to act by release of this information.
- The Department remains a preferred target for HVEs, and we are working with our partners in the intelligence and law enforcement communities, to include the FBI, to mitigate this risk.
- We can offer a classified briefing on the current threat if you are interested.

#### Counter-ISIL Emphasis Points

- These threats are typical of ISIL, illustrating their viciousness and desperation.
- These actions will not affect our resolve in the fight against ISIL, or our support for our partners.
- ISIL has managed to exploit open, commercially maintained information to target individuals, and has not breached secure Department websites or networks.
- We will not let ISIL to deter us, or our personnel, from using social media. To cut ourselves off from it would be to risk losing our share of the important public discussion about national security issues. No indication there was a data breach. It appears that the majority of information released in this list was obtained from open, commercially maintained information sites ("white page" sites, open-source government databases, etc.)

#### U.S. Northern Command Talking Points for Use During Media Interactions

- The safety of our service members is always a primary concern.
- We encourage our personnel to exercise appropriate OPSEC and force protection procedures.
- Services are conducting appropriate notifications in accordance with their service specific procedures.
- We are not going to further identify any specific service members on the list or where they are stationed.
- We are not going to discuss any specific force protection measures.
- We take all threats against service members seriously. Please look to the FBI for an assessment of the threat's credibility
- This page provides some general DoD guidance on social media:

<http://www.defense.gov/socialmedia/education-and-training.aspx/>

### **Navy Statement for Use with the Media**

"NCIS is actively evaluating this threat reporting and working with law enforcement and U.S. intelligence partners to address this incident. We have notified the affected Navy and Marine Corps service members and their family members as quickly as possible, in most cases in-person. In coordination with NCIS, we also provided guidance on personal protection and increasing their vigilance and awareness. NCIS continues to work with other agencies to reduce the effects of these threats."

### **Talking Points for Navy Leaders**

- Organizations friendly to the Islamic State in Iraq and the Levant (ISIL) [or as appropriate] continue to make names and addresses of our shipmates available to the public.
- While there is no evidence of operational planning or an imminent threat to these individuals, it is clear that the intent of this release of information is to cause concern and anxiety specifically for those on the list, their families and shipmates, and more generally to the force.
- Basic safety measures utilized to defend against violent crimes can also be useful to defend against a "lone wolf".
- Ongoing intelligence and law enforcement assessments continue to reinforce that sharing information smartly and with due caution remains safe. However, this incident reminds us of our personal responsibility for safety and operational security...stay aware, stay vigilant and be prudent about the information you share.
- The current guidance for our web pages, command social media, and engagement with U.S. and international media has not changed.
- We are committed to sharing new intelligence and updates with our Sailors and their families via appropriate command channels.

### **Draft Statement for Use with the Media Should Additional Names Be Released:**

- Unless there is evidence of an imminent threat, the U.S. Navy does not want to alert Sailors and their families to additional releases of information via the media. Initial notifications should be made through individual command channels, if at all possible. The Naval Criminal Investigative Service (NCIS) should be used as a back up to the command's efforts to communicate with its Sailors.
- The following statement should be used by U.S. Navy public affairs officers if queried by the media. "Organizations friendly to the Islamic State in Iraq and the Levant (ISIL) cause [or as appropriate] continue to make names and addresses of our shipmates available to the public. While there is no evidence of operational planning or an imminent threat to these individuals, it is clear that the intent of this release of information is to cause concern and anxiety specifically for those on the list, their families, and their shipmates. The U.S. Navy is notifying affected service members and their family members as quickly as possible. NCIS is actively evaluating this threat reporting and working with law enforcement and U.S. intelligence partners to reduce the effects of these threats."

**Draft Statement for use in the Aftermath of a Death or Injury of Navy Personnel Associated with the Release of PII.**

In the unlikely event that a death or injury occurs as a result of a PII release, law enforcement agencies will have the public affairs lead. The following statement is intended as a template when drafting a public statement following a tragic event. Details are quite likely to change given the exact nature of the event. It is important to note that DoD should not confirm the identities of the victims until the CACO process has run its course. DoD will be responsible to release the victim's names once next of kin notifications are complete. Questions beyond the scope of the following statement should be referred to law enforcement officials or CHINFO as appropriate.

- "The United States Navy is deeply saddened by the tragic events today at XXXXXXXX. Our thoughts and prayers are with the families of the victims (, the wounded,) and all those touched by this incident. There is little we can say at this point to alleviate the pain or answer the many questions this event raises, but we can pledge that the Department of Navy will do everything in its power to cooperate with the appropriate law enforcement agencies to hold those responsible accountable for this heart-breaking event.
- The identities of the victims cannot be confirmed until we have completed all of our next of kin notifications.
- The U.S. Navy is working with law enforcement and U.S. intelligence partners to evaluate how this event changes their assessment of the threat and what actions should be taken to safeguard others who have had their personal information released by organizations friendly to the Islamic State in Iraq and the Levant (ISIL) **[or as appropriate]**.
- The U.S. Navy is re-contacting these individuals and their families to ensure they are aware of the details of this development and are aware of the security measures being taken to protect them."

## **Sample Questions and Answers**

---

**Q: Is the Navy changing any of its policies and or procedures for personal online accounts due to this incident?**

A: The Navy has long advised Sailors and their families to be mindful about their disclosure of personal information on social media accounts. In addition, we train our Sailors about maintaining operational security.

**Q: Have all Sailors been notified about their status on the list?**

A: The U.S. Navy has contacted and discussed (or is in the process of contacting and discussing) this incident with all affected service members and their families.

**Q: What is the Navy doing about physical security for their personnel?**

A: The Navy annually requires all sailors to take refresher training in force protection measures regarding their personal safety. Sailors are trained to be vigilant about their surroundings.

**Q: How many Sailors were on the list posted on 21 March?**

A: There were a total of 41 Sailors and Marines on the list.

**Q: Is this a credible threat to Sailors and Marines?**

A: I'm unable to confirm the credibility of the threat and refer you to OSD Public Affairs for that information. However, in general, we work closely with law enforcement to assess any possible threat to our service members. We take all potential threats seriously and continue to actively assess this incident to insure the safety of our service members. It is important to remember, basic safety measures utilized to defend against violent crimes can also be useful to defend against a "lone wolf" terrorist.

**Q: Are the Sailors on the list connected to the ISIL bombing campaign conducted over the summer by USS Carl Vinson?**

A: We are unable to confirm how or why the Sailors who appear on the list were selected.

**Q: Is the list accurate?**

A: We are unable to confirm the accuracy of the entire list. I would refer you to OSD Public Affairs.

## **Follow-on Support**

---

During initial notification, a follow-on briefing will be offered. If desired, the follow-on briefing should be scheduled as soon as practicable but not less than 72 hours after initial notification.

The follow-on briefing team should consist of:

- A command representative
- Command Antiterrorism Officer (ATO)
- Law enforcement support (NCIS, FBI, local law enforcement, or other as appropriate)

Follow-on briefs should be tailored to provide desired support, but should include:

- Antiterrorism awareness training availability for non-Common Access Card (CAC) holders
- Support / advice regarding social media footprint
- A review of Home and Family Security Tips
- Guidance on reporting of suspicious activity
- A review of the Individual Security Vulnerability Assessment Checklist to ensure that affected personnel understand how to use it to conduct a self-assessment

## Home and Family Security Tips

---

The following Home and Family Security tips are provided by NCIS.

You and your family members should always practice basic personal security precautions. Familiarize your family with the local terrorist and criminal threat and regularly review the protective measures and techniques listed below. Ensure everyone in your family knows what to do in case of emergency.

The Joint Staff Antiterrorism Electronic Library contains additional resources and planning guides that you may find helpful. Their website is available here:

[http://jko.jten.mil/courses/at1/courseFiles/resources/Antiterrorism Electronic Library.html](http://jko.jten.mil/courses/at1/courseFiles/resources/Antiterrorism_Electronic_Library.html)

### TIPS FOR THE FAMILY AT HOME

- Restrict the possession of house keys. Change locks if keys are lost or stolen and when moving into a previously occupied residence.
- Lock all entrances at night, including the garage. Keep the house locked, even if you are at home.
- Destroy all envelopes or other items that show your name, rank, or other personal information. Remove names and rank from mailboxes.
- Maintain friendly relations with your neighbors.
- Do not draw attention to yourself; be considerate of neighbors.
- Keep yourself informed via media and internet regarding potential threats.
- Develop an emergency plan and an emergency kit, including a flashlight, battery- operated radio, first-aid kit including latex gloves, and copies of important personal documents including key points of contact.

### BE SUSPICIOUS

- Be alert to public works crews and other individuals requesting access to your residence; check their identities through a peephole and always contact the parent company to verify employee status before allowing entry.
- Be cautious about peddlers and strangers, especially those offering free samples. Do not admit salespersons or poll takers into your home.
- Watch for unfamiliar vehicles cruising or parked frequently in the area, particularly if one or more occupants remain in the vehicle for extended periods.
- Write down license plate numbers, makes, models, and colors of suspicious vehicles.
- Note descriptions of occupants.
- Report any suspicious videotaping/photography or unusual accommodation requests.
- Report any unattended bags or objects.
- Treat with suspicion any inquiries from strangers concerning the whereabouts or activities of family members.

- Report all suspicious activity to military police, security forces, or local law enforcement as appropriate.

#### TELEPHONE SECURITY

- Post emergency numbers on the telephone and pre-program phone numbers where possible.
  - Military Police/Security Forces:
  - Local Police:
  - Fire Department:
  - Hospital:
  - Ambulance:
- Do not answer your telephone with your name and rank.
- Report all threatening phone calls to security officials and the telephone company.
- Attempt to ascertain any pertinent information about the caller to include background noise, accent, nationality, or location.

#### SPECIAL PRECAUTIONS CONCERNING CHILDREN

- Never leave young children alone or unattended. Be certain children are in the care of a trustworthy person.
- If it is necessary to leave appropriately aged children at home (consistent with local laws and any additional command guidance), keep the house well lighted and notify a trusted neighbor.
- Instruct children to keep doors and windows locked and to not allow strangers inside.
- Teach children how to contact the police or neighbor in an emergency.
- Ensure children know where and how to contact parents at all times.
- Maintain recent photographs of your children. The photographs should display a clear view of the child's head.
- If you have children entering the home alone, teach them not to enter the home if the door is ajar, if a strange car is in the driveway, or if something else does not seem right. Tell them where they need to go if this situation occurs.
- Instruct your children to:
  - Never leave home without telling you where they will be and who will accompany them.
  - Travel in pairs or small groups.
  - Avoid isolated areas.
  - Use locally approved play areas where recreational activities are supervised by responsible adults and where police protection is readily available.

- Refuse automobile rides from strangers and refuse to accompany strangers anywhere on foot even if the strangers say mom or dad sent them, or said it was “okay.” Children should similarly be aware of strangers offering gifts, food, or using small animals to get them into a vehicle.
- Report immediately to the nearest person of authority (parent, teacher, or police) anyone who attempts to talk to or touch them in any way that makes them feel uncomfortable or scared.
- Never give information about family members over the phone, e.g., parent’s occupation, names, or future family plans and dates.
- Screen phone calls through voice mail to avoid answering calls from strangers.

#### **SECURITY PRECAUTIONS WHEN YOU ARE AWAY**

- Leave the house with a lived-in look (i.e. cut the grass and trim hedges before leaving).
- Stop deliveries of newspapers and mail or forward to a trusted neighbor’s home.
- Mail can also be held at the post office.
- Do not leave notes on doors or indicate the length of absence on telephone voicemail or electronic mail account.
- Do not hide keys outside the house.
- Use a timer to turn lights on and off at varying times and locations.
- Consider leaving the radio and lights on.
- Hide valuables.
- Notify the police or trusted neighbor of your absence.
- Ask a trusted friend or neighbor to check the residence periodically.

#### **VEHICLE SAFETY**

- Always lock your car.
- Park your car in well-lighted areas. Do not leave your car on the street overnight, if possible.
  - Check for suspicious persons before exiting the vehicle. If in doubt, drive away.
  - Leave only the ignition key with parking attendant, not residential keys. Use a “valet key” if available
  - Do not leave garage doors open or unlocked.
- Use a remote garage door opener if available. Enter and exit your car in the security of the closed garage. Remove garage door opener if car is left with service or repair shop.
  - Avoid displaying decals identifying the owner as military member.
- Make a habit of checking the vehicle and surrounding area before using your vehicle. If you find something out of the ordinary, DO NOT TOUCH IT. Contact the local authorities to report your findings.
- Consider varying routes to work and home and avoid late-night travel when possible.

- Consider carrying a cell phone in your vehicle.
- Plan your route and pre-plan alternate routes in case of emergency. Avoid isolated roads or dark alleys when possible.
- Know the location of all emergency services along your route.

## Operations Security Guidance for Family Members

---

There are many countries and organizations that would like to harm Americans and degrade U.S. influence in the world. It is possible and not unprecedented for spouses and family members of U.S. military personnel to be targeted for intelligence collection. This is true in the United States and especially true overseas. Family members play a crucial role in ensuring safety just by protecting known information about military day-to-day operations. Understanding critical information and identifying the methods adversaries use to collect this information is vital to the success of the Operations Security (OPSEC) program.

**Be Alert.** Foreign governments and organizations can collect significant amounts of useful information by using spies. A foreign agent may use a variety of approaches to befriend someone and get sensitive information. This sensitive information can be critical to the success of a terrorist or spy and, consequently, deadly to Americans. Their methods have become very sophisticated. The Internet has become the preferred method of gathering information. Family members may unwittingly provide all the necessary information to compromise the military members' mission.

**Be Careful.** There may be times when the military spouse cannot talk about the specifics of his or her job. It is very important to conceal and protect certain information such as flight schedules, ship movements, temporary duty locations, and installation activities, just to name a few. Something as simple as a phone discussion concerning where the military spouse is going on temporary duty, or deploying to, can be very useful to U.S. adversaries.

**Protect Critical Information.** Even though this information may not be classified, it is what the Department of Defense calls "critical information." Critical information deals with specific facts about military intentions, capabilities, operations, or activities. If an adversary knew this detailed information, U.S. mission accomplishment and personnel safety could be jeopardized. It must be protected to ensure an adversary does not gain a significant advantage. By being a member of the military family, some bits of critical information might be known. Do not discuss them outside of the immediate family and especially not over the telephone or through e-mails. Be careful of the information shared on social media, such as Facebook and Twitter.

- Examples of Critical Information
  - Detailed information about mission of assigned units.
  - Details concerning locations and times of unit deployments.
  - Personnel transactions that occur in large numbers (e.g., pay information, power of attorney, wills, or deployment information).
  - References to trend in unit morale or personnel problems.
  - Details concerning security procedures.
  - Family members' personal information.

**Puzzle Pieces.** These bits of information may seem insignificant. However, to a trained adversary, they are small pieces of a puzzle that highlight what U.S. forces are doing and planning. Remember, the elements of security and surprise are vital to the accomplishment of U.S. goals and collective DoD personnel protection.

Where and how you discuss this information is just as important as with whom you discuss it. Adversary's agents tasked with collecting information frequently visit some of the same stores, clubs, recreational areas, or places of worship as you do. If anyone, especially a foreign national, persistently seeks information, notify the authorities immediately.

## Individual Security Vulnerability Assessment Checklist

---

This vulnerability assessment checklist was provided by NCIS to evaluate residences. Prospective renters should attempt to negotiate security upgrades as part of the lease contract when and where appropriate.

### Exterior Grounds:

- If you have a fence or tight hedge, have you evaluated it as a defense against intrusion?
- Is your fence or wall in good repair?
- Are the gates solid and in good repair?
- Are the gates properly locked during the day and at night?
- Do you check regularly to see that your gates are locked?
- Have you eliminated trees, poles, ladders, boxes, etc., that may help an intruder to scale the fence, wall, or hedge?
- Have you removed shrubbery near your gate, garage, or front door that could conceal an intruder?
- Do you have lights to illuminate all sides of your residence, garage area, patio, etc.?
- Do you leave your lights on during hours of darkness?
- Do you check regularly to see that the lights are working?
- If your residence is guarded, does his/her post properly position him/her to have the best possible view of your grounds and residence?
- If applicable, does your guard patrol your grounds during the hours of darkness?
- If applicable, has your guard been given verbal or written instructions and does he/she understand them?
- Do you have dogs or other pets that will sound an alarm if they spot an intruder?
- Have you considered installation of a camera system with recording capabilities or a dummy camera system as a deterrent?

### Interior Features:

- Are your perimeter doors made of metal or solid wood?
- Are the doorframes of good solid construction?
- Do you have an interview grill or optical viewer in your main entrance door?
- Do you use the interview grill or optical viewer?
- Are your perimeter doors properly secured with good heavy-duty deadbolt locks?
- Are the locks in good working order?
- Can any of your door locks be bypassed by breaking the glass or a panel of lightwood?
- Have you permanently secured all unused doors?
- Are your windows protected by solid steel bars, ornamental, or some other type of shutters?
- Are unused windows permanently closed and secured?
- Are your windows locked when they are shut?

- Are you as careful of second floor or basement windows as you are of those on the ground floor?
- Have you secured sliding glass doors and similar style windows with a broom handle, "charlie bar," or good patio door lock?
- If your residence has a skylight, roof hatch, or roof doors, are they properly secured?
- Does your residence have an alarm system?
- Have you briefed your family and household assistants on good security procedures?
- Do you know the phone number of the police or security force that services your neighborhood?

**General:**

- Are you and your family alert in your observations of persons who may have you under surveillance or who may be casing your house in preparation for a burglary or other crime?
- Have you verified the references of your domestic help, and have you submitted their names for security checks?
- Have you told your family and household assistants what to do if they discover an intruder breaking into or already in the house?
- Have you restricted the number of house keys?
- Do you know where all your house keys are?
- Have you identified telephone contact numbers for all adults?
- Have you identified rally points, such as at a neighbor's house or other identified location, for use in emergencies if the house must be evacuated?